Identity management of e-ID, privacy and security in Europe

de Hert, P.J.A.

Published in:
Information Security Technical Report

Publication date:
2008

Document Version
Publisher's PDF, also known as Version of record

available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodinf.htm

Information Security Technical Report

Identity management of e-ID, privacy and security in Europe. A human rights view

Paul De Hert[a,b]

[a]*Law Science Technology & Society (LSTS), Department of Metajuridica, Faculty of Law, Vrije Universiteit Brussel, Brussels, Belgium*
[b]*Tilburg Institute for Law, Technology and Society, University of Tilburg, Netherlands*

ABSTRACT

With privacy enhancing identity management, end users are given better ways for managing their identities for specific contexts. One could easily argue that the need to implement identity management systems that are privacy enhancing follows from the EU data protection regulation. One of the challenges while developing privacy enhancing identity management is getting governments to become genuinely interested, both in their capacity of data processing organisation and legislator or policy maker. Another challenge, this time for the private sector, is to find the right balance between data protection perfection and simplicity or users' convenience, while developing privacy enhancing identity management systems. After a brief discussion of these challenges we discuss the growing human rights recognition of the value of digital identity and its management. In particular, the German constitutional court seems to pave the way for a basic right to have digital identity protected and secured.

1. General

Privacy is generally associated with the protection of the integrity, autonomy and private life of the individual. Basically, it's about people's right to choose how they want to live their life, and what things they want to keep private. Do we have a choice when interacting online? Often we do. The emergence of the Internet has allowed more and more people to discover certain aspects of identity formation hitherto unknown. Online worlds let you create a character, a home and a new personality if you wish. Often we do not. In order to obtain certain goods or services we are required to identify ourselves in ways beyond our control.

Identity management (IDM) is commonly referred to as the set of processes and tools that serve to establish the identity of a user (e.g. enrol an employee, customer, contractor) in a system.[1] Today a trend towards user-centricity and privacy enhancing identity management is noticeable,[2] with the EU funding research initiatives such as *Prime* enabling more user control.[3] User-centricity distinguishes itself from other

E-mail address: paul.de.hert@uvt.nl

[1] A. Carblanc, 'Digitial identity and its management in e-society', paper presented at NATO Advanced Research Workshop (ARW) on Identity, Security And Democracy; Social, Ethical and Policy Implications of Automated Systems for Human Identification (Ait) organised by the Centre for Science, Society and Citizenship and the Israeli Center for the Study of Bioterrorism in Jerusalem, September 2–4, 2006 (9p.), p. 3.

[2] S. Clauss and others, 'Privacy-Enhancing Identity Management', *IPTS reports*, 2002, vol. 67 (http://www.jrc.es/home/report/english/articles/vol67/IPT2E676.htm).

[3] Jan Camenisch and others, 'Privacy and identity management for everyone,' *ACM*, 2005, p. 20–27. For a more comprehensive oversight, see Martin Meints & Marit Hansen, 'Identität – die europäische Perspektive. Übersicht über aktuelle EU-Projekte', *DuD – Datenschutz und Datensicherheit*, vol. 30 (2006) Issue 9, p. 531–532.

1363-4127/$ – see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.istr.2008.07.001

notions of IDM by emphasising that the user (or some agent of the user) – and not some authority – maintains control over ''what, where, when, and to whom'' a user's identity information is released.[4] The researchers gathered in *Prime* to develop identity management systems that give individuals sovereignty over their personal data so that: (1) individuals can limit the information collected about them by using pseudo-identities, certifications and cryptography when performing online transactions; (2). individuals can negotiate legally binding ''privacy policies'' with their service providers which govern how disclosed personal data can be used and which precautions must be taken to safeguard it, and (3) individuals and service providers can use automated mechanisms to manage their personal data and their obligations towards data which they have collected from other parties.[5]

The proposed system includes an anonymous credential system, an access control system based on a novel paradigm, a negotiation functionality, and an automated reasoning system. ''This machinery performs most of the decision making involved in privacy management and involves the user mainly for making final high-level decisions and for giving consent to data processing. Together, these components give a user the power to easily manage her privacy without being an expert in the field''.[6]

2. The legal framework

With privacy enhancing identity management, end users are given better ways for managing their identities for specific contexts. One could easily argue that the need to implement identity management systems that are privacy enhancing follows from the EU data protection regulation, in particular EU Directives 95/46/EC and 2002/58/EC (whose purposes are to safeguard individuals' privacy and freedom) and from the EU 2000 Charter on Fundamental Rights. These sets of regulations impose a number of important principles:

(1) the purpose limitation principle – data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer;
(2) the data quality and proportionality principle – data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed;
(3) the transparency principle – individuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country, and other information insofar as this is necessary to ensure fairness;
(4) the security principle – technical and organisational security measures should be taken by the data controller that are appropriate to the risks presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process data except on instructions from the controller;
(5) the rights of access, rectification and opposition – the data subject should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her.

There is no question about the ability of identity management systems to support the realisation of data protection rights and goals geared towards giving a person notice, consent, security, and access with respect to his personal data. In identity management systems it is, for example, technically possible for parties to provide the type of notice and negotiate the kind of consent envisioned in the principle of purpose limitation. Similarly, identity management systems can include mechanisms to provide users with security as spelled out in the principles of security and to enable a person to know how data is treated and contest that treatment, as foreseen by the principles of rights of access, rectification and opposition.[7]

3. Problems with privacy enhancing identity management: public sector

One of the challenges while developing privacy enhancing identity management is getting governments to become genuinely interested, both in their capacity of data processing organisation and legislator or policy maker. Governments have traditionally had a central role in providing for the identity of citizens through the issuance of documents such as birth and death certificates, passports, social security numbers or driving licences. Today they need to be concerned over respect for privacy, data protection and security and respond to challenges posed by digital identity management by setting up frameworks that are beneficial to user control over e-Identity aspects. The OECD has elaborated guidelines to improve a culture of security between all the stakeholders involved in the exchange of information and to encourage sound security practices.[8] The EU launched a *Safer Internet Action Plan*,[9] and both at the level of the Council of Europe and at the level of the EU measures were adopted obliging Member States to incriminate certain crimes related to digital identity and to collaborate in cases

[4] Mary Rundle and others, 'At a Crossroads: ''Personhood'' and Digital Identity in the Information Society', *STI Working Paper 2007/7*, OECD, February 2008 (52p.), p. 22 (http://www.oecd.org/dataoecd/31/6/40204773.doc).

[5] Jan Camenisch and others, 'Privacy and identity management for everyone', ACM, 2005, p. 20.

[6] Jan Camenisch and others, 'Privacy and identity management for everyone', ACM, 2005, p. 20.

[7] Mary Rundle and others, 'At a Crossroads', p. 33. Mary Rundle and others, 'At a Crossroads', p. 28–32.

[8] OECD, *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* (adopted as a Recommendation of the OECD Council at its 1037th Session on 25 July 2002), Paris, OECD, 29p (http://www.oecd.org/dataoecd/16/22/15582260.pdf).

[9] See http://ec.europa.eu/information_society/activities/sip/index_en.htm.

with an international dimension.[10] The EU 2002 Directive on Privacy and Electronic Communications requires that location information generated by mobile phones can only be further used or passed on by network operators with prior user consent, unless it is an emergency call. In a recent report commissioned by the OECD examples are forwarded of user-centric and privacy enhancing approaches to national identity card schemes.[11] In the future the Belgium e-Identity card will allow persons to prove that they are older than 18 without being required or forced to make public other data.[12]

A 2003 European report showed with regard to identity theft in Europe that, due to strong existing European legislation, which defines clear privacy and data protection rights, this type of crime is less frequent than in other countries.[13] Clearly, our policy makers are not absent. However, some governments are setting up very simple, centralised identity management systems using unique identifiers ignoring risks and security risks.[14] Currently all European Member States are setting up centralised or semi-centralised fingerprint databases of citizens, largely ignoring the sloppy, insecure use of fingerprint biometrics in the private sector.[15] In June 2007 Dutch scientists have discovered that a certain type of smartcard, Mifare, which is used to gain access to government departments, schools and hospitals around Britain, is carrying a serious security flaw that allows it to be easily copied.[16] Earlier this year a major smartcard system with similar goals in the Netherlands was easily compromised by the same investigators.[17]

The government is also responsible for national security and criminal law enforcement. The law acknowledges this and allows, for example, use of data without consent for these purposes.[18]

However, on response to the threat of terrorism after the tragedy of September 11, many governments enhanced their surveillance powers, voting laws that were heavily criticised from a privacy perspective. The EU seemingly takes part in the global tendency towards ambient intelligence security enforcement scenarios, relying on the massive collection and processing of (personal and non personal) data in combination with data mining and profiling techniques. This tendency highlights the fragility of data protection law as a tool to control surveillance. Lawful collection and processing of personal data does not prevent *per se* unethical practices deployed in the name of security, or unjust decisions based on them. Arguably, the alleged need 'to mobilize information to prevent terrorism'[19] and equivalent instructions frontally contradict fundamental principles of data protection law (such as the minimisation principle) and the requirements for privacy enhancing identity management.[20] A general framework to limit surveillance needs to be designed, in which the enabling force of data protection regulation is complemented with more clearly defined restrictive principles.

4. Problems with privacy enhancing identity management: private sector

Turning to the private sector we see a major challenge in finding the right balance between data protection perfection and simplicity or users' convenience, while developing privacy enhancing identity management systems. Without this balance users will consent to schemes that are simple but erode privacy concerns.

In a 2008 OECD report these and other risks are amply identified.[21] The report insists on the following technical qualities that users are implicitly demanding for the privacy aspects of user control: decentralisation (maximal decentralisation of identity information into as many separate data contexts as possible); data minimisation and selective disclosure; use of local identifiers (avoid using more global identifiers such as a government tax identity number); verifiability (the system must support mechanisms for verification of claims), and composability. Even more important in the report is the suggestion to rewrite five data protection principles

[10] P. De Hert, G. González Fuster & E.-J. Koops, 'Fighting cybercrime in the two Europes: the added value of the EU Framework Decision and the Council of Europe Convention', *International Review of Penal Law*, vol. 77, 2006, No. 3–4, 503–524.

[11] Mary Rundle and others, 'At a Crossroads', p. 36.

[12] See 'Algemeen EID Officieel antwoord van KUL onderzoeksgroep op artikel en studie Persbericht – De Elektronische Identiteitskaart is Veilig', COSIC, K.U. Leuven, 13 June 2008 (http://belsec.skynetblogs.be/post/5966749/eid-officieel-antwoord-van-kul-onderzoeksgroe).

[13] B. Clements, I. Maghiros, L. Beslay, C. Centeno, Y. Punie, C. Rodrïguez & M. Masera (eds.), *Security and Privacy for the Citizen in the Post-September 11 Digital Age. A prospective overview*, Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), July 2003, Brussels, European Commission, IPTS-Technical Report Series, EUR 20823 EN, 188p. (http://ftp.jrc.es/EURdoc/eur20823en.pdf).

[14] A. Carblanc, 'Digitial identity and its management in e-society', p. 3.

[15] P. De Hert, 'Legal Aspects of Biometric Technologies', in Institute For Prospective Technological Studies – Joint Research Centre, *Biometrics at the Frontiers: Assessing the Impact on Society*, Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), February 2005, IPTS-Technical Report Series, EUR 21585 EN, p. 75–85.

[16] Miller, Vikki, ''Oyster card: fears over Mifare security'', *The Telegraph*, 21 June 2008. http://www.telegraph.co.uk/news/newstopics/politics/2168791/Oyster-card-fears-over-Mifare-security.html.

[17] 'OV-chip 2.0. Dutch develop open source smart card for public transport', Amsterdam, June 19, 2008, http://www.nlnet.nl/press/20080619-ovcard.html.

[18] Article 13 of the EU 1995 Directive contains exceptions with regard to the purpose limitation principle, the transparency principle and the principle of access.

[19] See, for instance: Markle Foundation Task Force (2006), *Mobilizing Information to Prevent Terrorism: Accelerating Development of a Trusted Information Sharing Environment*, Third Report, July.

[20] F. González Fuster, S. Gutwirth & P. De Hert, 'The Role of Law, Ethics and Justice in Security Practices' in J. Peter Burgess & David Rodin (eds.), *The Role of Law, Ethics and Justice in Security Practices Conference report*, Oslo, International Peace Research Institute (PRIO), 2008 (69p.), 22–24 (http://www.prio.no). On the risk of destruction of personhood, see Mary Rundle and others, 'At a Crossroads', p. 21.

[21] Mary Rundle and others, 'At a Crossroads: ''Personhood'' and Digital Identity in the Information Society', *STI Working Paper 2007/7*, OECD, February 2008, 52p (http://www.oecd.org/data-oecd/31/6/40204773.doc).

mentioned *above* in order to lend better support to emergent privacy enhancing identity management systems based on user control.[22] Complementing existing formulation of data protection principles is needed. These principles 'have a strong focus on protecting a person's data against inappropriate treatment by other actors; however, they place the individual in a rather passive role and so fail to provide him with the proactive right to use his own identity information as he sees fit. The law may need to lend its support to emergent IDM tools so that the user will by default have a right to make use of his personal data' (p. 28). These and other recommendations to adapt the existing legal framework will not only benefit the end user, but equally governments that have a duty to respect fundamental rights and producers that need to be aware of the existing legal framework. At the present stage there are too few indications about business' readiness to come up with services or processes that live up to higher data protection concerns.[23] The importance of consent in user-centricity is beyond doubt but it is only one necessary ingredient of privacy-enhancing identity management.

Currently many organisations believe that they own the personal information of their clients. A change in business thinking and culture is needed towards a business model in which the individual is perceived as the ultimate owner of their own information.[24] The current data protection framework is not of a nature to oblige the business community to seek for best data protection standards, as long as the processing of data is based on consent. The active duty to explore emerging concepts for IDM such as user-centricity and user-control cannot be enforced in an unequivocal way. Data protection regulation does not prohibit, as such, organisation-centric business models. Even the recent recognised 'fundamental right to data protection' in the EU Charter on Fundamental Rights[25] does not explicitly infer a duty to develop user controlled identity management systems to protect better data protection aspects of e-Identity.

5. A fundamental right to the confidentiality and integrity of information systems

The future identity infrastructure will not be simple. In a world of ''Internet of things'', computing will ''melt invisibly into the fabric of our business, personal and social environments, supporting our economic, health, community and private life.''[26] More data will be generated and the management of it will become unthinkable without a proper legal and technological infrastructure. Carblanc advocates a holistic approach and stresses the need to involve all stakeholders when elaborating a framework and guiding principles.[27] Without denying the business interests in reducing costs and enhancing user convenience and governmental interests in law enforcement and fraud detection, it is useful to end with an observation about the growing human rights recognition of the value of digital identity and its management. In particular, the German constitutional court seems to pave the way for a basic right to have digital identity protected and secured. On 15 December 1983, in the *Volkszählungsurteil*[28] the Court recognised a right to self-determination based on the *allgemeines Persönlichkeitsrecht*, as protected by Article 1 (Human Dignity) in conjunction with Article 2 (Right of Liberty) of the German Constitution. The Court related that the individual needs ''be protected from unlimited collection, storage, use, and transmission of personal data as a condition of the development of his or

[22] Mary Rundle and others, 'At a Crossroads', p. 28–32.

[23] See for example, The European e-Business report 2006–07 (www.ebusiness-watch.org/key_reports/documents/EBR06.pdf). In this document privacy is mentioned only twice and data protection only once.

[24] ''At present, most organisations view every client contact as an opportunity to begin building an ongoing relationship with the client. This relationship may lead to more opportunities to do business with the client or to build client satisfaction and loyalty. Consequently, the company seeks to gather information from an individual the first time he requests a service, with a view to building an ongoing relationship. This orientation may lead a company to gather information that is not strictly required for the transaction, and it may prevent the company from deleting information once the transaction is completed. A shift would not mean that organisations could not build client relationships; it would just mean that they would have to do so through explicit relationship-building transactions to which the individual would consent. Organisations must come to see that the personal information of their clients is not only an asset, but also a potential liability, e.g. a source of law suits over the failure adequately to protect such data, particularly in the absence of a client driven/consented reason for having it. As regulatory controls over personal information increase, the amount of liability associated with data collection will also force companies to re-evaluate their data gathering and retention requirements. Despite the human tendency to want to know the identity of the individual being served, for many situations this may not be necessary and may not be desired by the individual. To process transactions with little or no identifying information will often mean reliance on a third party assertion or assurance on behalf of the individual. This will require an enterprise not only to be confident in the technical trust assurances (e.g. digital certificates) provided, but also to develop new business and operational relationships with those third parties. This may include regular assurances/audits of third parties and co-operation in trouble-shooting and investigations'' (Mary Rundle and others, 'At a Crossroads', p. 24).

[25] Cf. Charter of Fundamental Rights of the European Union of the European Parliament, December 7, 2000, *O.J.*, No. C 364, 2000, p. 1 and fol. In this Charter, a separate right to data protection is recognised next to the right to a private life for the individual. Article 7 of the Charter recognises a right to privacy. Article 8 of the Charter focuses on the protection of personal data: 'Everyone has the right to the protection of their personal data. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to their data, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority' (Article 8 EU Charter).

[26] John Backley, Policy framework paper presented at workshop ''From RFID to the Internet of things'', 6 and 7 March 2006, CCAB, Brussels, final report. Available at http://www.rfidconsultation.eu/docs/ficheiros/WS_1_Final_report_27_Mar.pdf.

[27] A. Carblanc, 'Digitial identity and its management in e-society', p. 6.

[28] *BVerfGE* 65 E 40.

her free personality under the modern conditions of data processing''. With unequalled precision, the Court of Karlsruhe explained in detail the shift of power that takes place whenever the state or private actors interact with an individual through ICTs. The Constitutional Court reasoned that a person's knowledge that his or her actions are being watched inevitably curtails his or her freedom to act.

As recently as 27 February 2008, the German Constitutional Court gave a ruling about the constitutionality of secret online searches of computers by government agencies.[29] It considered those searches to be contrary to a newly recognised basic right, namely ''the right to confidentiality and integrity of information systems'' which complements the 1983 ''fundamental right to informational self-determination'' (see above). The court pondered that informational–technical systems, including laptops, PDAs and mobile phones 'alone or in their technical interconnectness […] makes it possible to get insight into relevant parts of the conduct of the life of a person or even gather a meaningful picture of the personality'. This affects the right to self-determination of the individual who might refrain, for instance, from opening a web-blog or disseminate emails.

The Court limits exceptions to the right to specific cases where exist ''factual indications for a concrete danger'' for the life, body and freedom of persons or for the foundations of the state or the existence of human beings, and declares that state spying measures can only be implemented after approval by a judge. Moreover, secret online searches must in any case be constrained by ad hoc technical measures not to interfere with ''the core area of the conduct of private life''. This landmark ruling, that recognises a citizen's right to the integrity of their information-technology systems and introduces elements of user-centric identity management (safeguards against (subsequent) misuse through technology and the intervention of judges), can potentially be as influential as the 1983 recognition by the same Court of the ''right to informational self-determination''.

[29] Published on 27 February 2008 (*OnlineDurchsuchung*, 1 BvR 370/07; 1 BvR 595/07).